Before the
National Telecommunications and Information Administration
United States Department of Commerce

Development of the Nationwide Interoperable Public Safety Broadband Network	)))	Docket No. 120928505–2505–01

COMMENTS OF RESEARCH IN MOTION LIMITED

Paul Lucier
Vice President
Government Solutions
Research In Motion Limited
Office: 519-888-7465
E-mail: plucier@rim.com

November 7, 2012

TABLE OF CONTENTS

Before the
National Telecommunications and Information Administration
United States Department of Commerce

Development of the Nationwide Interoperable Public Safety Broadband Network	)))	Docket No. 120928505–2505–01

COMMENTS OF RESEARCH IN MOTION LIMITED

As a global provider of mission-critical data services whose offerings rely on the interconnection of more than 650 network partners, Research In Motion Limited ("RIM") understands well the challenges and opportunities facing FirstNet in its effort to develop the FirstNet Nationwide Network ("FNN"). RIM is pleased to provide comment on the conceptual network architecture presentation made at the FirstNet Board of Directors' September 25, 2012 meeting.[1] As detailed below, the company supports the Proposal's core features and offers recommendations as to how the Proposal might be augmented. RIM stands ready to work in partnership with FirstNet as it develops and implements the FNN.

INTRODUCTION

RIM revolutionized the mobile industry with the introduction of the BlackBerry® solution in 1999. Since then, RIM's business has centered on the provision of state-of-the-art device-to-device communications services. RIM has excelled in support of those clients requiring particularly secure and reliable communication.

---

[1] F. Craig Farrill, First Responders Network Authority Presentation to the Board: FirstNet Nationwide Network (FNN) Proposal, Sept. 25, 2012 ("Proposal").

RIM is extremely proud of and protective over its longstanding partnership within the public-safety sector – dating back to the introduction of the BlackBerry in 1999 – and considers this relationship to be essential to its long-term success. In fact, many of the company's device management policies were created to satisfy the needs of its federal, state, and local government customers. To this day, thousands of first responders and public safety workers around the world utilize BlackBerry hardware, software and infrastructure to conduct their mission-critical duties.[2]

Given the company's experience in this arena, RIM is excited for the opportunity to play a substantial role in the design and implementation of the FNN. RIM's service offerings are built on seven key foundations, each of which is central to FirstNet's success:

> **1. Security.** RIM is the internationally uncontested leader in providing secure end-to-end network communications based upon a virtually impenetrable global infrastructure. Strong security protocols are built into RIM's devices and its network. Such security protocols are central to the achievement of the FNN's objectives: First responders must be able to rely on the FNN during times of emergency, and that network must not be susceptible to intrusion by those who would do harm to the nation.
>
> **2. Reliability and Redundancy**. The RIM network is comprised of a Multiprotocol Label Switching ("MPLS") backbone, Relay message-passing switches, and a private data "cloud" for applications hosting. This network is globally distributed among world-wide data centers and managed by two fully redundant Network Operations Centers ("NOCs"). RIM's network is connected to hundreds of mobile network operators and regional Internet Service Providers ("ISPs") via firewalled and load-balanced connections. RIM utilizes advanced Authentication, Authorization and Accounting ("AAA") functionality embedded in the network and on RIM's BlackBerry smartphones and tablet devices. At present, RIM's MPLS network offers 99.994% availability, and its Relay infrastructure offers 99.97% availability.[3] All major systems in RIM's data centers are architected for disaster recovery.

---

[2] For specific case studies on BlackBerry Public Safety solutions please refer to http://us.blackberry.com/business/industry/public-safety.html?LID=us:bb:business:industries:publicsafety&LPOS=us:bb:business

[3] The availability numbers are 2012 year-to-date averages through mid October 2012.

3. Ubiquity. RIM currently has contractual and operations relationships connecting more than 650 partners in 175 countries. RIM's Customer Service Operations supplies multiple-language help desk and deep technical support worldwide to enterprise customers, mobile operators and consumers alike. The ability to coordinate multiple networks in multiple regions is also critical to the FNN's success, because (as discussed below) the FNN will be most robust if it relies on a network of networks, drawing on existing facilities where possible.

4. Scalability. RIM serves approximately 80 million global subscribers, approximately 60 million BlackBerry Messenger users, and has more than 200,000 BlackBerry Enterprise Servers deployed. Its network carries 31 petabytes of secure data traffic per month. For perspective, one petabyte of data is the equivalent of watching HD video for 13 years and four months. RIM's global network is designed for scalability at all levels. The FNN must also, of course, be scalable, capable of serving law enforcement and other first responders across the nation.

5. Interoperability. As noted, the BlackBerry network connects more than 650 network partners. To do so, the company employs specialized carrier interface platforms that account for the specific needs of the myriad platforms used by RIM's customers. When a device roams across different mobile network types or carriers, RIM's network shifts to maintain its affiliation with the device. On the services side, RIM's network provides access via its proxies to external Web sites, email and IM services, in addition to secure connectivity behind the firewall to enterprises. RIM's interface platforms are continuously modernized and honed to provide the optimal user experience from any wireless network.

6. Efficiency. RIM's devices and network infrastructure are designed to minimize the use of spectrum through compression techniques and data routing protocols that allow our devices to continue to operate efficiently during times of high network congestion, e.g. the Washington D.C. earthquake, 9/11 or Hurricane Katrina.

7. Open Application Development. RIM has developed a dynamic and vibrant mobile application development ecosystem to support millions of BlackBerry consumer and enterprise users across the globe. It employs open standards to promote third-party applications development, and supports applications designed for alternative platforms. Thousands of developers take advantage of RIM's application-development framework to create high-value applications to suit the needs of communications-service consumers of all types.

As detailed below, RIM supports the FNN conceptual framework detailed by the Proposal. A distributed, multi-carrier network of networks will best promote the public interest and the public-safety community. Moreover, the impediments to a multi-provider network are

not as severe as it might seem. Indeed, RIM has itself addressed and surmounted those same challenges in developing and deploying its own network, and looks forward to utilizing its expertise to facilitate deployment of a robust and dynamic FNN.

I. RIM'S SUPPORT FOR THE PROPOSED FIRSTNET NATIONWIDE NETWORK CONCEPTS

Although RIM could support any of the three "network options" addressed by the Proposal , we believe that a "Diverse Nationwide Network with Multiple Wireless Networks and Systems"[4] would be the most effective way to meet FNN's goals and objectives. As the Proposal indicates, only this approach can provide near-ubiquitous network coverage and the flexibility associated with network redundancy. The proposed FNN architecture seeks to provide nationwide wireless services to the U.S. first-responder community and their respective safety agencies. The best way to accomplish this goal would be to leverage new and existing networks, technologies, and relationships among wireless service providers, wireline broadband providers, state/local/tribal authorities, device manufacturers, and application developers. This goal is achievable provided FirstNet relies on experienced vendors and suppliers with a proven track record of delivering services across a multi-vendor/multi-provider infrastructure.

Moreover, the potential drawbacks of such an approach cited in the Proposal – "[m]ore complex business relationships" and "[n]ew implementation of existing technologies" – are easily surmounted. As detailed above, RIM has itself managed business relationships with more

[4] Presentation at 8.

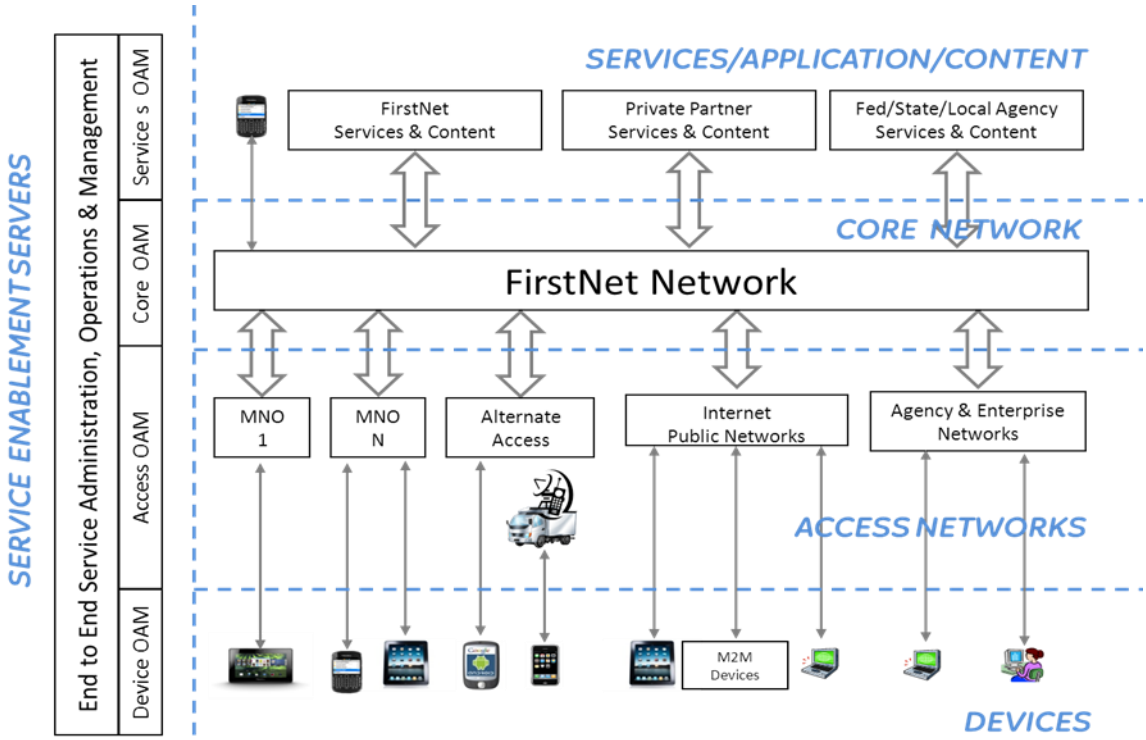
than 650 network partners worldwide, coordinating an interoperable network linking its approximately 80 million global subscribers to one another and to individuals using other platforms. Likewise, in a fast-changing communications environment, providers such as RIM must routinely pursue "[n]ew implementation of existing technologies." After introducing the world to the smartphone 13 years ago, RIM has evolved to respond to a broad array of customer demands, by providing solutions from point-to-point messaging to online video to social networking to a variety of hosted services provided over the secure BlackBerry network.

II. FNN ARCHITECTURAL ISSUES AND CHALLENGES

A. Overview of the FNN Architecture

RIM envisions the FNN architecture as shown in the below figure, which builds upon the diagram provided in the Presentation:[5]

[5] Presentation at 18-19.



As depicted, RIM proposes that the FNN conceptual framework be modified to include a Service/Application/Content layer and a Service Enablement/Operations, Administration & Management ("OA&M") vertical tier. These additions help to more fully capture an end-to-end service perspective. The new services layer is the layer at which services, applications, or content would be located. Services could be provided by FirstNet; private partners; federal, state, or local agencies; or some combination of those entities. Each service would be expected to provide its own authorization at this layer, relieving the FirstNet core of the responsibility to authorize private partner or other third-party services.

The new end-to-end service enablement/OA&M tier would communicate with the service enablement and management functions of each layer. The service enablement/OA&M tier would perform functions such as registration; security; AAA services; configuration; provisioning; policy management; service and system measurement, monitoring, data collection,

and analysis; and archiving. RIM recommends that transport of administrative, signaling and control message channels comprising the OA&M tier be segregated from the user/media channels to avoid the possibility that user/media data congestion could prevent command and control functions and to enhance security of the FNN.

B. The Evolved Packet Core Network

RIM supports the proposed use of an evolved packet core ("EPC") network architecture at the heart of the FNN.[6] Under this approach, the FNN would utilize a single packet-based core architecture in place of a dual system of legacy circuit-switched communications and packet-switched services. RIM agrees that the use of a single EPC will enable FirstNet to support innovative new services and applications, leaving it better able to serve the needs of first responders not only today, but also into the future.

C. The FirstNet Service Delivery Platform

Because the FNN infrastructure must support a multi-service platform, RIM encourages FirstNet to adopt a holistic, service-oriented view that looks beyond traditional voice, video, and messaging silos. Rather, the FNN must be configured to promote next-generation applications that combine and leverage these traditional services to bring the best in new technology to first responders. Such applications could – along with other content – be hosted in a managed "FirstNet Service Cloud," much in the way that RIM ensures quality and security by hosting its

---

[6] See Proposal at 13-19.

own branded services. Alternatively, such services, applications or content could reside with a carrier partner or within federal, state, or local agency networks. More than likely, the FNN would rely on a combination of such architectures, depending on the service and the capabilities of the parties involved.

1. Voice

The FNN should obviously support voice communications. Voice services could be routed through the FNN EPC but would be compatible with existing mobile telephony networks, and would leverage carriers' existing and planned LTE or cellular networks. FirstNet could also serve as its own inter-exchange provider for first-responder voice services. The FNN should also support voice messaging services leveraging existing "Push to Talk" technologies, as well as support secure voice capabilities. Secure Voice can be enabled on this network by installing proxy servers behind the firewall, which then would serve as a midpoint between end devices allowing for end-to-end encryption of the voice call. It is important, however, that voice services (and, indeed, all services associated with the FNN) be provisioned in a user-friendly manner; otherwise, they are likely to go unused.

2. Data

FNN also must support traditional data services, including messaging, email, large file transfers, web based services, and multimedia. In addition, FNN should offer services that facilitate applications using real-time media streaming. Real-time maps and geolocation data are especially critical to many first responders. Audio/video conferencing will likely require dedicated conferencing technology, which also could be installed within the FirstNet architecture itself.

FirstNet should also support near real-time push notifications, on both a one-to-one and one-to-many basis. This would enable "channel owners" to disseminate vital information to a large number of first responders in a highly efficient "broadcast mode" to keep responders informed. This technology is readily available and used by RIM's BlackBerry Messenger ("BBM") services.

FirstNet should also consider enabling direct client-to-client data connectivity to allow for peer-to-peer applications or direct content sharing, which could help reduce network congestion during times of emergency.

3. Operations, Administration and Management

Drawing from RIM's experience managing a global network, we recommend that FNN consider supporting a variety of administrative, signaling and control messages to facilitate emergency communications. These include system and infrastructure commands, provisioning and configuration data, distribution of application software updates, event and management data, and authentication services.

OA&M communications are likely to be critical to the FNN's success in managing the provider/vendor environment and supporting multiple services with different underlying delivery requirements. OA&M communications will be needed to facilitate coordination among providers and to ensure quality of service ("QoS"); admission control, service prioritization, pre-emption policies and signaling schema, and performance, latency and error allocations across multiple suppliers.

4. Security Services

FNN and the connected devices must keep FNN content and services secure. RIM envisions that FirstNet devices would isolate FirstNet connectivity, limiting the accessibility of

the FNN to approved applications and approved users. Eligible FNN users and applications could be authorized to access all FNN functions and/or communications streams, or could be limited to a subset of FNN's functionalities.

RIM notes that strong security functionality is rendered even more critical in light of the grave cybersecurity threats faced by the United States. As Secretary of Defense Leon Panetta emphasized last month, terrorists and other entities have long been "probing America's critical infrastructure networks, targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country."[7] FirstNet must ensure that the nation's enemies are not able to spy on it through its public-safety network, or to thwart that network during times of emergency, when Americans will need it most.

5. Other

In addition to the above, FirstNet should consider a variety of other functionalities that could be very valuable to first responders. For example, closed user groups ("CUGs") or user community functionality would allow network owners to deliberately partition groups of users at the logical layer of the network. For example, in the case of three simultaneous events in different parts of the nation, the use of CUGs could ensure that responders enjoy access to services relevant to their particular event without being burdened by traffic relating to another emergency elsewhere. As importantly, such a partition would provide additional protection for sensitive information germane to a particular event response or personally identifiable

---

[7] *See* Secretary Leon Panetta's Speech About Cybersecurity (Oct. 12, 2012), *available at* http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262.

information (e.g. medical records). It would also alleviate network traffic by limiting distribution of information to relevant users. CUGs therefore could streamline the administration and management of network use, and improve responsiveness to particular emergencies.

Similarly, the ability to collect and archive event and audit information can be useful. First responder practices, processes and procedures can be improved through the analysis of this event and audit data.

D. The Role of Devices within the FNN

FirstNet cannot adequately address network design without considering interactions between the network and connected devices. Specifically, FNN-compatible devices will need to meet a number of essential criteria, and these criteria should be considered as the FNN is designed. For example, FNN-enabled phones will need the ability to attach and interoperate with a variety of different mobile network technologies and WiFi networks. They will also need to support a broad mix of primary and roaming bands (including 700 MHz LTE) within compact mobile form factors. FNN devices must offer strong endpoint security from the device through to a secure back end enterprise network, and must be able to effectively and securely hand off sessions between various types of wireless networks.

Much of device capability is driven by the mobile operating system ("OS") running the device. Any FNN OS should support secured tunnels to end point devices with strong authentication mechanisms; the ability to channel data traffic from devices to specified data networks to segregate particular types of traffic for routing, QoS, and billing purposes; the ability

to support common applications across a variety of multi-carrier networks; and effective modern user interfaces that permit effective operation within an emergency-response environment.[8]

The devices used on the FNN must also be subjected to the highest possible security standards. FirstNet should likewise ensure that devices that do not meet certification standards or pose potential security risks are not used as endpoints in the FNN.

III. PROMOTING THE DEVELOPMENT OF ROBUST FNN-CAPABLE APPLICATIONS

As one of the earliest builders of a framework for the development, purchase, and deployment of smartphone applications, RIM offers the following thoughts on how FirstNet can successfully operate a framework for public safety applications.

A. Suggestions for Applications that Would Benefit Public Safety Users

Across the public safety sector, users are seeking tools that facilitate collaboration and information distribution. FirstNet applications that help fill this need would be of great value. For example, one application might use social-networking features to enable the ad-hoc creation of a group, or virtual "team room." Such features would ideally provide the ability to invite users to the group and use collaboration tools such as file sharing, team and peer-to-peer messaging/audio/video, GPS tracking, and conferencing system integration. Virtual groups or

[8] RIM has a long history of providing devices and mobile operating systems with these capabilities and more than three billion app downloads to date. We would be glad to serve as an advisor to FirstNet and its partners to meet the needs of FirstNet users.

team rooms could be used for short-term purposes, such as emergency response, or for long-term projects, such as ongoing brainstorming or planning for an organizational unit.

Another potentially useful application would enable users to subscribe to pushed or broadcast files, messages, videos, alerts, etc., from a centralized service or individual. End users could use such applications to make sure they have the information they need without having to individually locate and retrieve it. These applications could integrate the incoming messages into a user's inbox so that the notifications are part of their central communication flow.

While neither FirstNet nor RIM could possibly anticipate all the useful applications that will emerge on FirstNet, RIM's experience with mobile devices and applications has yielded several best practices that FNN applications developers and devices makers should strongly consider:

(1) **Integrate applications.** The integration of applications into a mobile device's native communications tools provides the most effect experience for the end user. RIM recommends that applications integrate functionalities as fully as possible by, for example, leveraging the contacts application for communication purposes, using the native calendar application for conferencing and scheduling, and utilizing native instant messaging and peer-to-peer applications for coordination and communication.

(2) **Support and take advantage of multi-threaded execution.** It is vital that the FNN platform supports multitasking, so that multiple applications can be used in parallel. Not only does this enable applications to interact, but it also ensures that applications need not be closed or suspended because of an incoming call or the need to look up information in another application. Requiring a user to end a session in an

application prematurely because of a limitation of the platform would hinder the utility of the application and the device to public-safety personnel.

(3) Correctly handle connectivity interruptions. Because applications will often be required to function in areas of poor, unreliable and/or intermittent network connectivity (*e.g.*, in the field during a natural disaster), it is imperative that platforms support, and applications take advantage of, out-of-the-box handling of unreliable network connectivity, intelligent routing, reliable transport protocols, compression and error mitigation technologies.

B. Specific Security Requirements for FNN-Capable Applications

RIM believes the best approach for FNN security is to formulate a tiered rating for the security requirements of different groups and different types of data. However, a base level of security is necessary for all FNN communications. RIM recommends the use of National Institute of Standards and Technology-approved algorithms, such as end-to-end 256 bit AES encryption of data-in-transit and data-at-rest. RIM also recommends that FirstNet choose a standard user authentication mechanism, which should include two-factor authentication for at least some types of data. Third, RIM recommends that the system authenticate endpoints to guard against device ID spoofing.

C. Encouraging the Development of High-Quality Applications

There are several steps FirstNet can take to encourage the development of high-quality applications:

Embrace standards-based development. FirstNet should commit to standards-based development tools and languages (such as HTML5, JavaScript and CSS3). Use of open standards will promote reuse of code functions and services, ensure cross-platform support, adapt to future interface options and help to ensure the development of "future-proof" applications for emerging platforms. Interface requirements should include the capability to handle audio/video and standard file types, securely store such data, and run multiple applications in parallel so that urgent information and communication can be presented as soon as relevant.

Establish a global directory across FirstNet. FirstNet could also promote applications development by creating a centralized, global directory of network endpoints and devices. Due to users and devices (including smartphones, tablets, printers, vehicle-based endpoints, etc.) being dispersed but very often needing to address groups or contact various endpoints quickly, this global directory should include an entry for every endpoint, and contact information (email address, phone number, IP address, or similar) for each endpoint. The directory would contain the properties of these endpoints and devices, such as the kinds of hardware, operating systems, security requirements, and first responder functions, agencies or departments. The list of these properties would provide focus to the software development community in suggesting and developing applications relevant to the various user groups.

Create a centralized code-sharing library. Applications often include features already incorporated into other applications. A code-sharing library would allow developers to post functions they have written for reuse by other developers and applications, eliminating the need for them to expend resources rewriting existing features. The success of code sharing would, of course, rely on the previously advocated commitment to standards-based development languages such as HTML5.

Centrally hosted shared services. There is great benefit in hosting shared services in a centralized location, permitting applications to call upon certain commonly used functionalities. For example, hosting a file sharing/storage service would mean that any developer that desires a file-sharing feature for an application could leverage the existing service, instead of creating the entire service anew. Centrally hosted shared services also help ensure compliance with requirements regarding security, auditing, and management; because the single shared service can be tested instead of each individual application. Examples of useful shared services include file upload/download/sharing, team and peer-to-peer messaging/audio/video, GPS tracking, and conferencing system integration.

D. Specific Suggestions for FirstNet's Applications Certification Requirements

RIM recommends several specific features for FirstNet's application certification process. First, the device platform(s) for FirstNet applications should meet minimum certification requirements such as FIPS 140-2 and Common Criteria. Next, application developers should utilize an internal code review to ensure compliance with specific requirements relating to endpoint API usage, minimum quality assurance, application integration, and proper and efficient use of shared services and functions. RIM also recommends that FirstNet explore the possibility of establishing a third-party certification regime in order to ensure an unbiased evaluation.[9]

---

[9] For further information see http://us.blackberry.com/business/topics/security/certifications.html

E. Delivery Methods under the FNN Conceptual Architecture Model

RIM recommends that FirstNet design the FNN so that applications may be "pushed" over an encrypted wireless channel to FNN endpoints and automatically installed without user intervention. Any application delivery solution should also provide the ability to wirelessly deliver a version upgrade to an existing application on the endpoint. It should also provide full management control of the application and the application data, including the ability to reliably remove the application and application data remotely, with confirmation that application and application data were removed successfully.

IV. CONCLUSION

RIM appreciates the opportunity to comment on the conceptual framework for the FNN and welcomes the opportunity to help address this most pressing public safety need. RIM's extensive experience in delivering assured services over a platform similar to the network envisioned by FirstNet leaves it especially well positioned to serve as a partner in the conceptualization and development of the FNN. The company looks forward to collaborating with other stakeholders to quickly and efficiently make the nationwide interoperable public safety network a reality.

Respectfully submitted,

Paul Lucier
Vice President
Government Solutions
Research In Motion Limited
419 Philip Street
Waterloo, Ontario
Canada N2L 3X2

Office: 519-888-7465
E-mail: plucier@rim.com

November 7, 2012